RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: CLS-R03

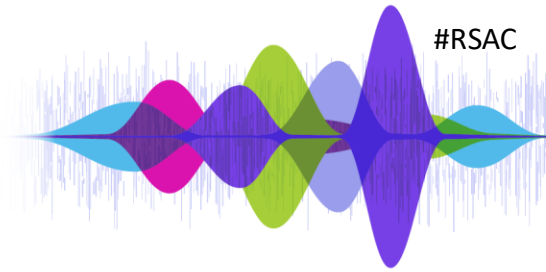
Standardizing a Privileged Access Model for a Multi-Cloud Environment

Rupanjana Mukherjee

Principal Security Architect
Google
https://www.linkedin.com/in/rupanjana-mukherjee/

Jon Sabberton

Senior Manager
Google
https://www.linkedin.com/in/jonsabberton/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

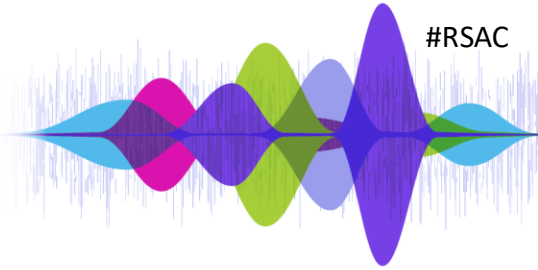
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Case studies and examples are drawn from our experiences and activities working for a variety of our clients, and do not represent our work for any one client or set of clients.

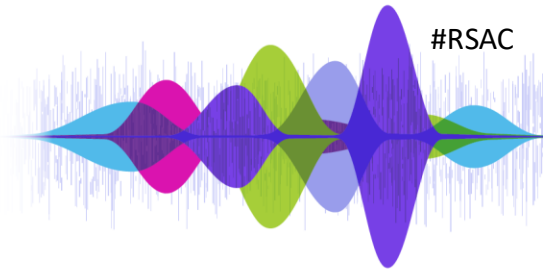
In many cases, details have been changed to obscure the identity of our clients and individuals associated with our clients.

© Google Cloud - Mandiant



Objectives

- Understand importance of tiering for cloud environments
- Attack surface analysis for multi-cloud hybrid environment
- How the Tier Model for Multi-Cloud protects from cyber attacks
- Securing the multi-cloud environment using tiering architecture



Agenda

- Analysis of risks in Multi-Cloud environments
- Attack scenarios in Multi-Cloud environments
- Introduction to Tier Model for Multi-Cloud environment
- How Tier Model controls protects from attacks
- Google – Mandiant approach to remediate hybrid environments
- Key takeways

RSAC 2025 Conference

Analyzing the risks with Multi-Cloud

Who does this apply to?

99% of organizations are running some sort of hybrid infrastructure (cloud + on-prem).

State of Cloud Threat Detection and Response Report - March 2023

How the attacks have evolved

2019-2021: Focus on Ransomware

During this period, there was a rise in ransomware facilitated by the growing availability of Ransomware as a Service offerings

2022 onwards: Shift to Data Theft + Extortion

During this period, ransomware began to lose ground to **data theft** and **extortion** as the primary driving factor for financial success

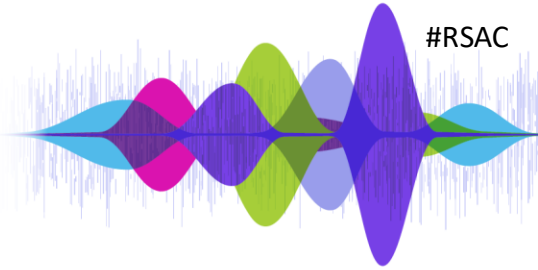
Increase in intrusions involving data theft:

29% - 37%

2021 2024

M-Trends 2024

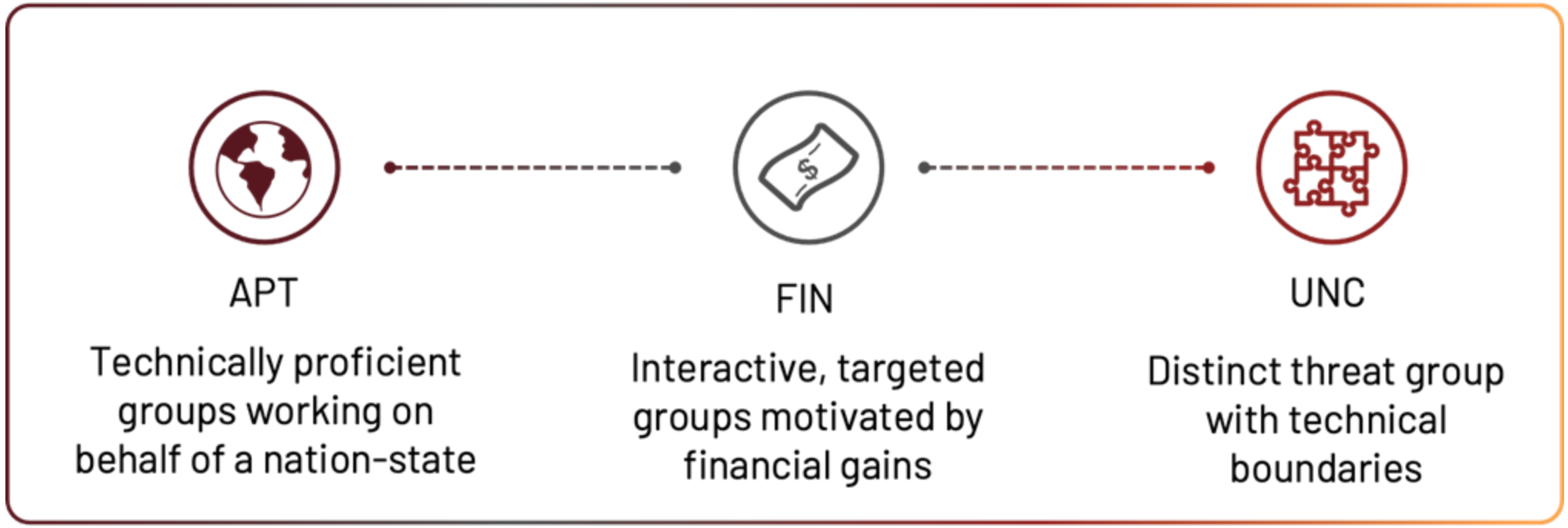
What has Changed?



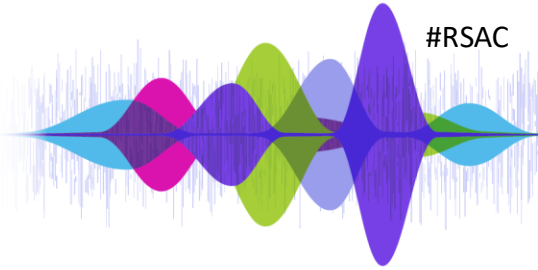
Organizations have migrated critical workloads to the cloud; however, they have not adapted their security mindset to this new landscape

- Lines between on-premise and cloud environments are blurred
- Extended attack surface
- Risk of third-party and external access
- Attacks are multi-dimensional

Threat Actor Categorization


APT
Technically proficient groups working on behalf of a nation-state
FIN
Interactive, targeted groups motivated by financial gains
UNC
Distinct threat group with technical boundaries

Challenges with Hybrid Multi-Cloud



- Multiple Identity planes
- Lack of Network Segmentation
- Inconsistent security controls
- Abuse of Trust Relationships
- Consistent patching, monitoring and governance

RSAC 2025 Conference

Mandiant Case Studies

Elevating privileges across cloud and on-prem

UNC

1 Attacker registers |organization|-helpdesk.com & |organization|-sso.com

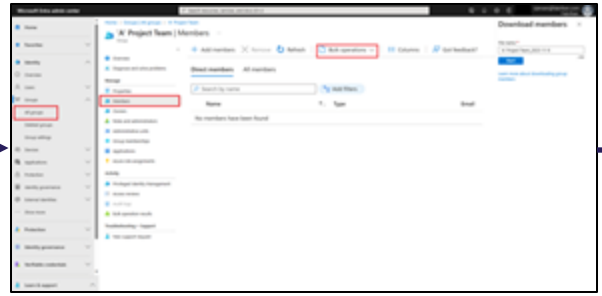
2 SMS-ishing Attack against users for credentials

3 A non-privileged user enters credentials.

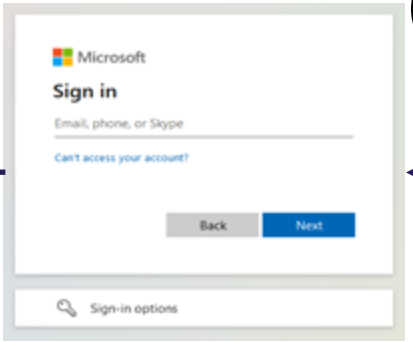
Attacker steals and replays token to log into Entra ID

4 Attacker logs into Entra ID and performs bulk user, group membership, and role assignment download

Entra ID



5 Password spraying attack against targeted and highly privileged admin accounts collected from Step 4



6 Azure Tenant Compromised

Successful login and MFA registration against two accounts.

Account 1 is a break glass account assigned Global Admin role in Entra ID.

Account 2 is a PAM admin.

7 Attacker registers virtual machine within Entra ID.

Then logs into Defender to whitelist malware (RATs).

Logs into Intune to deploy malware across fleet of endpoints.

8 Uses malware backdoor and piggybacks VPN and accesses credential-vault using compromised Account 2 (PAM admin).

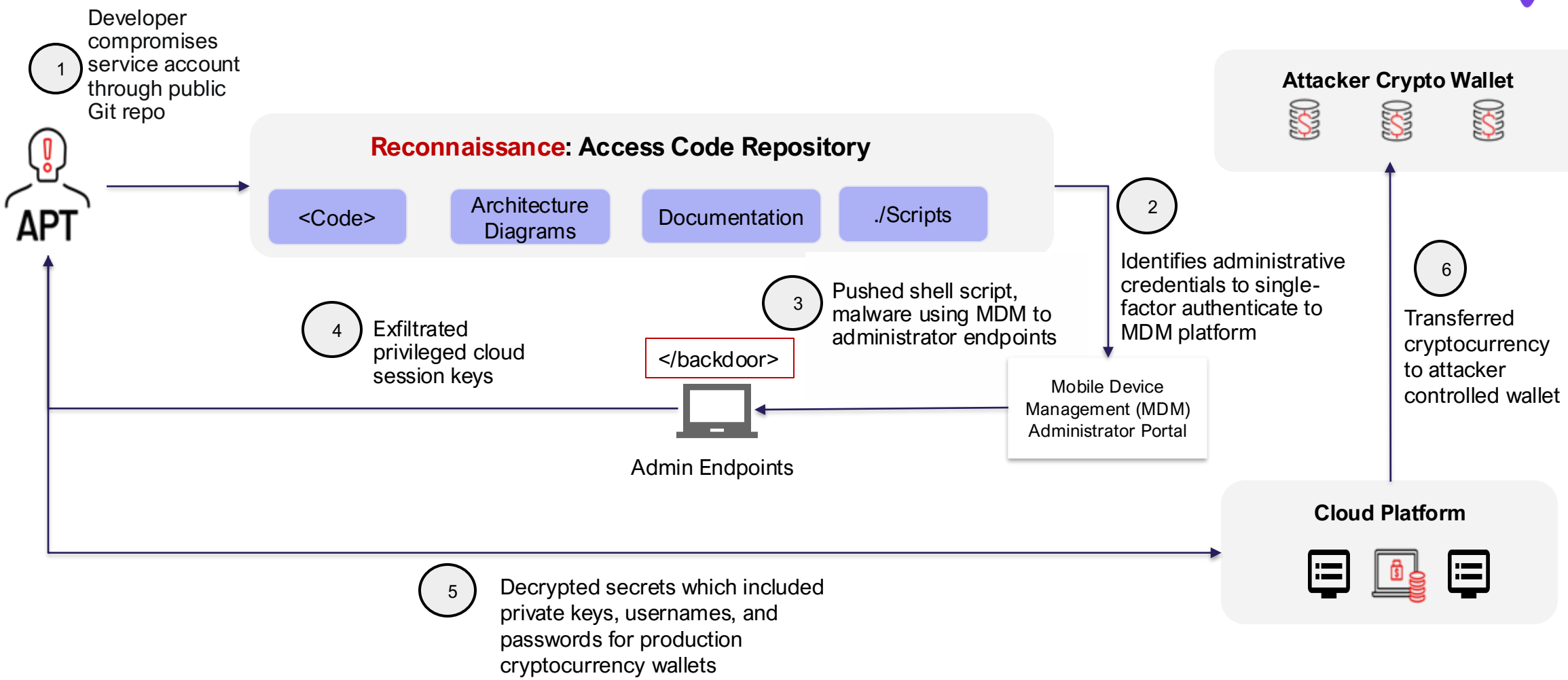
Retrieves Domain Admin and VMware Root account credentials in clear-text.

9 Total Domain Compromise + Data Loss

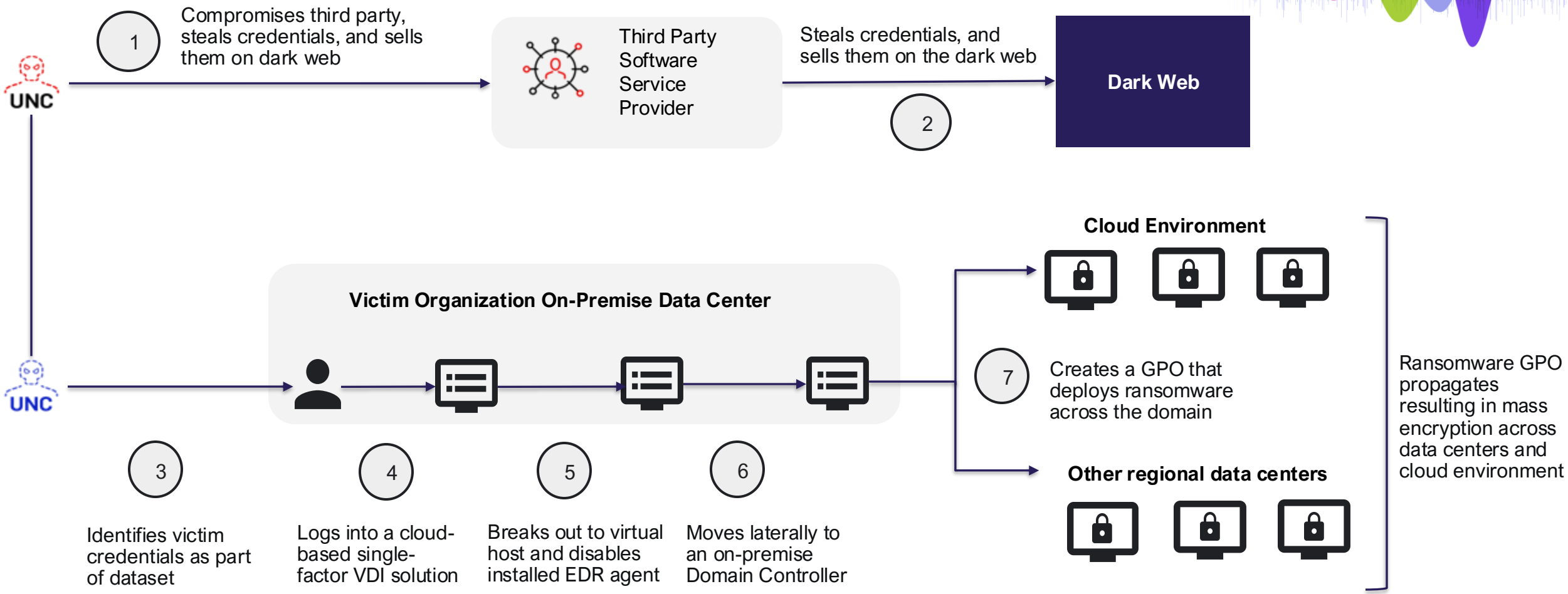
Moves laterally to on-premise AD; dumps the NTDS.dit.

Then, moves to VMware Infrastructure and encrypts production ESXi Hosts.

Abusing Management Tooling for Cloud Access



Third Party tooling to Cloud Compromise


1
Compromises third party, steals credentials, and sells them on dark web
UNC
Third Party Software Service Provider
Steals credentials, and sells them on the dark web
2
Dark Web
Cloud Environment
Victim Organization On-Premise Data Center
UNC
7
Creates a GPO that deploys ransomware across the domain
Other regional data centers
Ransomware GPO propagates resulting in mass encryption across data centers and cloud environment
3
Identifies victim credentials as part of dataset
4
Logs into a cloud-based single-factor VDI solution
5
Breaks out to virtual host and disables installed EDR agent
6
Moves laterally to an on-premise Domain Controller

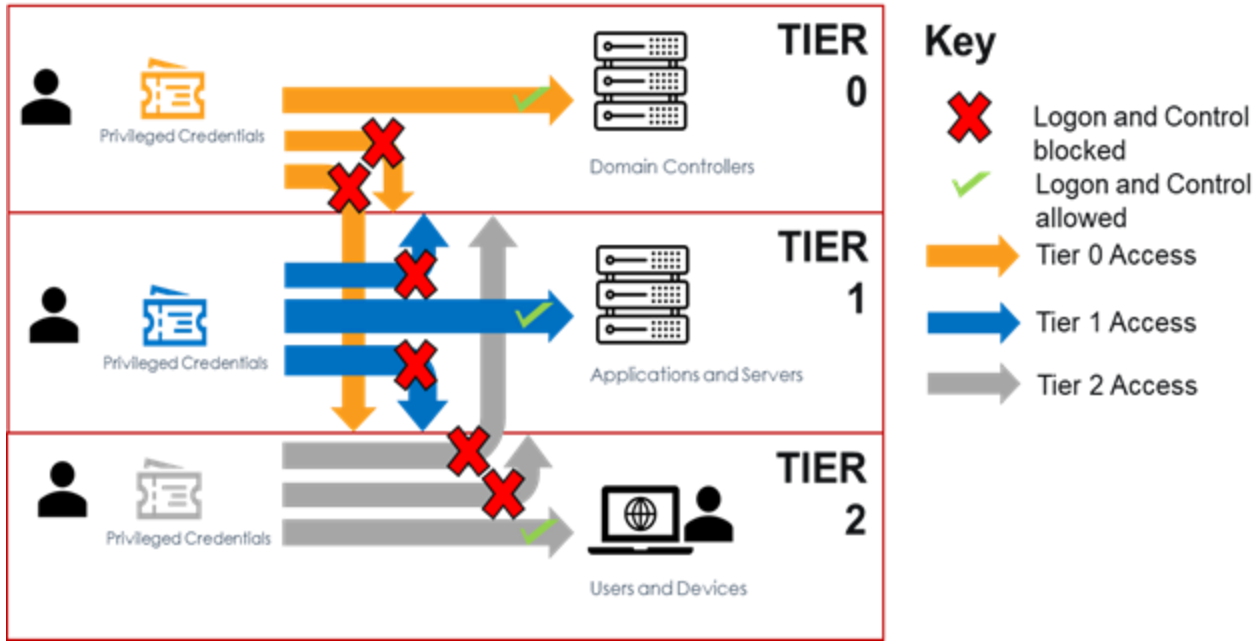
RSAC 2025 Conference

Attack Remediations - Tier Model for Multi-Cloud

What is Tiering?

Tiering is meant to segment and classify resources, data, users based on criticality and sensitivity.

Tiering helps protect against credential theft, lateral movement and privilege escalation.

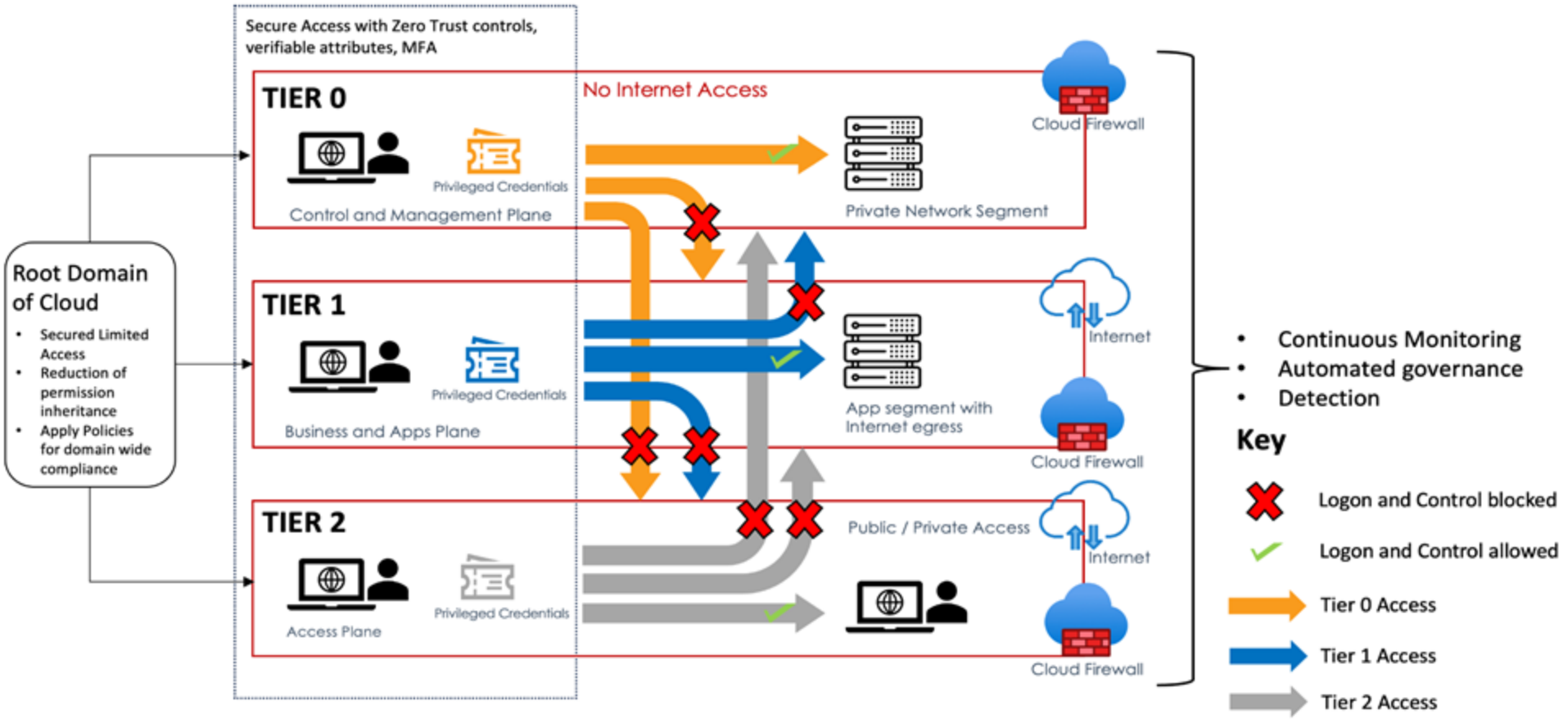


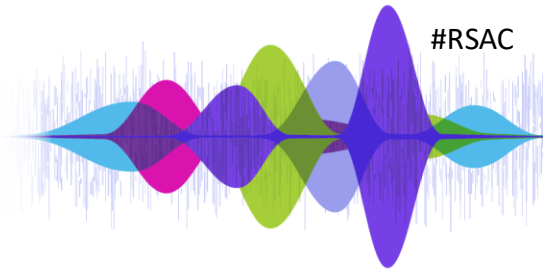
Define Tiering in the Cloud

Tier 0	**Trusted Services Infrastructure layer**	This tier comprises services and assets responsible for secure access. This includes the following: - IAM Services - PIM/PAM - Administrator Identities/Endpoints - Networking/ SD-WAN Administrator - Virtualization host for Tier 0 servers	**Why are these services Tier 0/highest criticality?** A breach in this tier can result in complete domain compromise.
Tier 1	**Business layer**	This tier consists of resources that host applications and intellectual property of the organization (corresponding IaaS and PaaS resources supporting the apps)	**Why are these services Tier 1?** A breach in this tier will compromise application/workload data restricted to that workload only.
Tier 2	**End User layer**	This tier enables end user access. - Virtual desktop environments - - End-User Identities/Endpoints - CIAM Tenant - Partner/Vendor Accounts	**Why are these services Tier 2?** A breach of an asset in this tier compromises a user and their data.

Cross-over paths between tiers could lead to an attacker elevating privileges

Applying Tier Model to Multi-Cloud





Harden critical/trusted service infrastructure

Protect Access

- Use credential tiering in multi-cloud.
- Cloud Administrators should use cloud-only accounts that are not tied to an on-premises/federated identity store.
- Use strong / phishing-resistant MFA methods.

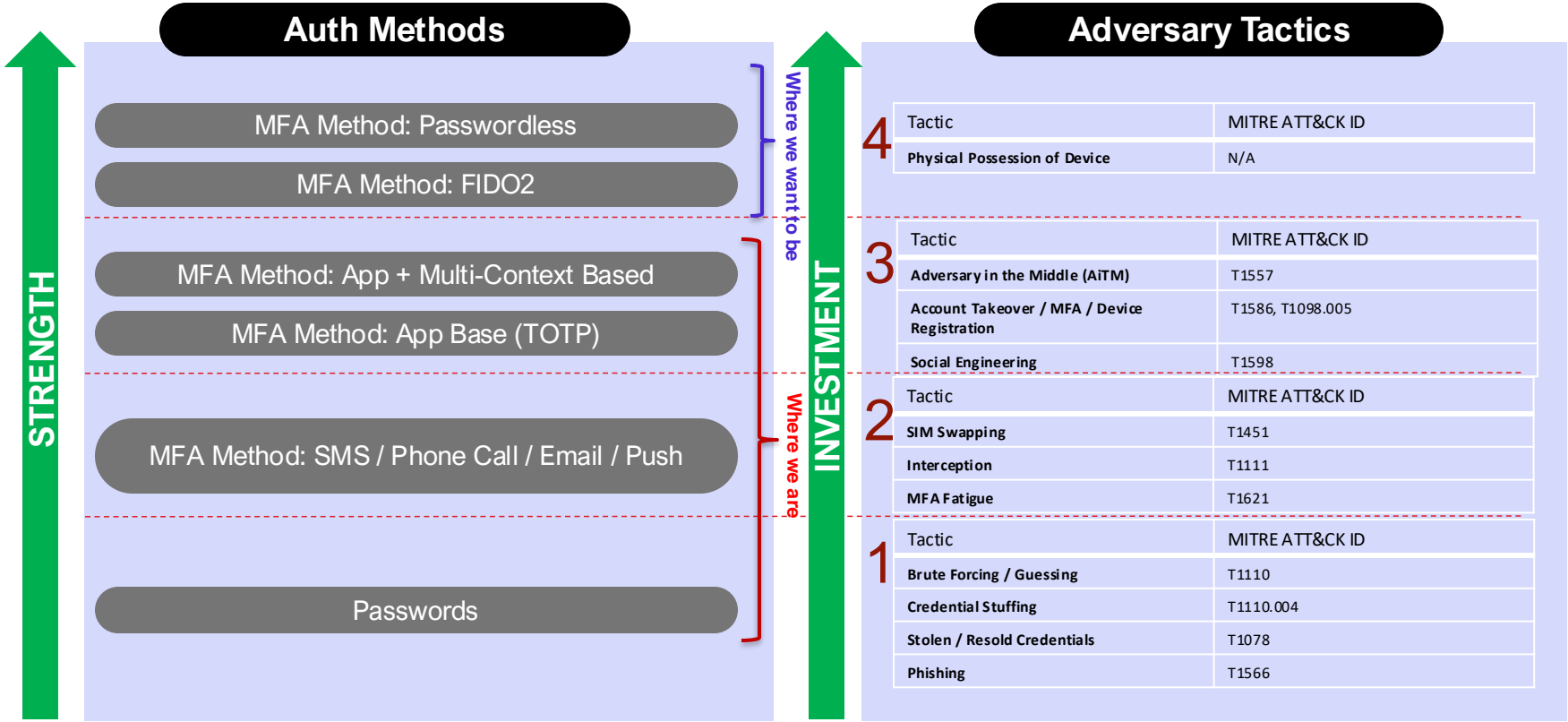
Segmentation

- Restrict access to critical resources and admin consoles from specific allow listed accounts, devices and networks.
- Segregate critical and non-critical resources – Apply resource tiering.

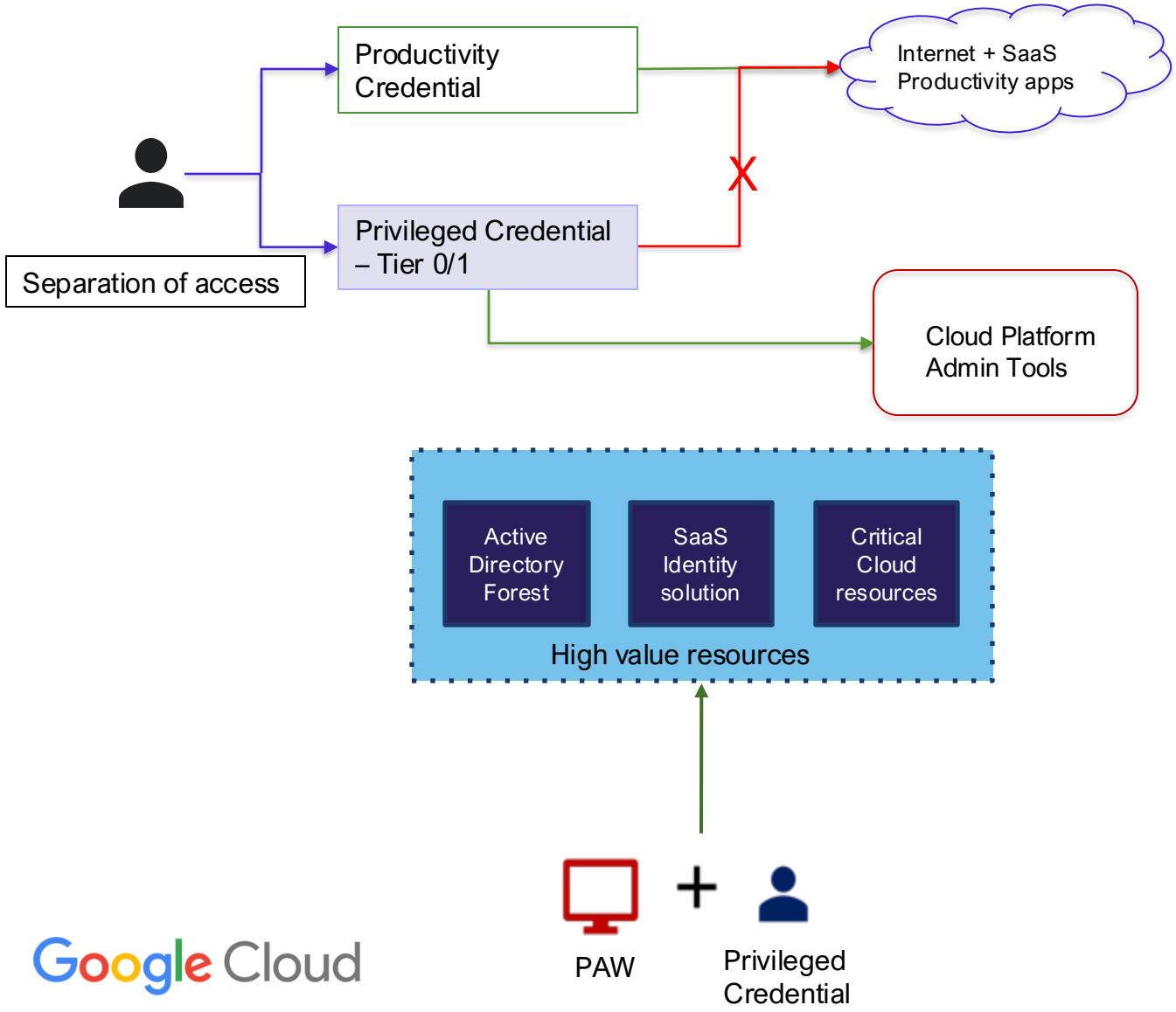
Proactive Detections

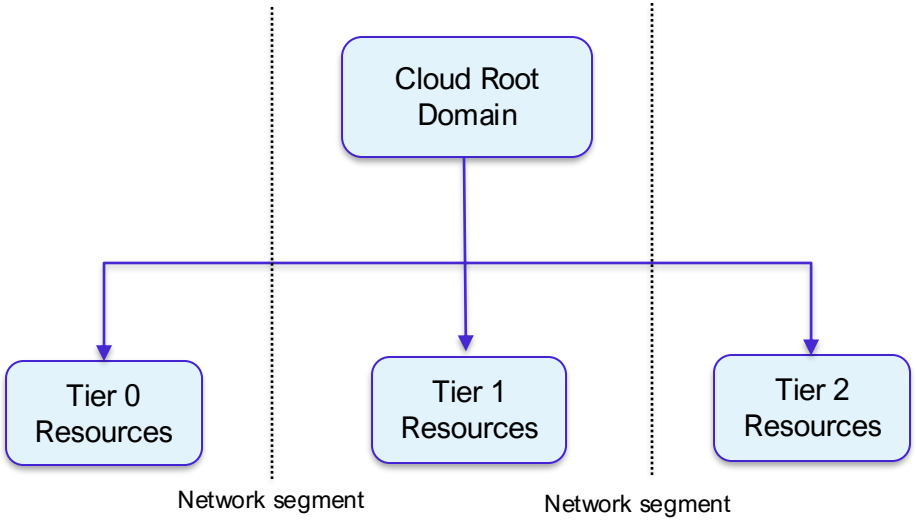
- Centralize logs from the control plane of trusted service infrastructure.
- Develop a baseline of normal activity and alert on deviations.

Multi-Factor Authentication Methods


Auth Methods
STRENGTH
MFA Method: Passwordless
MFA Method: FIDO2
MFA Method: App + Multi-Context Based
MFA Method: App Base (TOTP)
MFA Method: SMS / Phone Call / Email / Push
Passwords
Where we want to be
Where we are
INVESTMENT
Adversary Tactics
4
Tactic | MITRE ATT&CK ID
Physical Possession of Device | N/A
3
Tactic | MITRE ATT&CK ID
Adversary in the Middle (AiTM) | T1557
Account Takeover / MFA / Device Registration | T1586, T1098.005
Social Engineering | T1598
2
Tactic | MITRE ATT&CK ID
SIM Swapping | T1451
Interception | T1111
MFA Fatigue | T1621
1
Tactic | MITRE ATT&CK ID
Brute Forcing / Guessing | T1110
Credential Stuffing | T1110.004
Stolen / Resold Credentials | T1078
Phishing | T1566

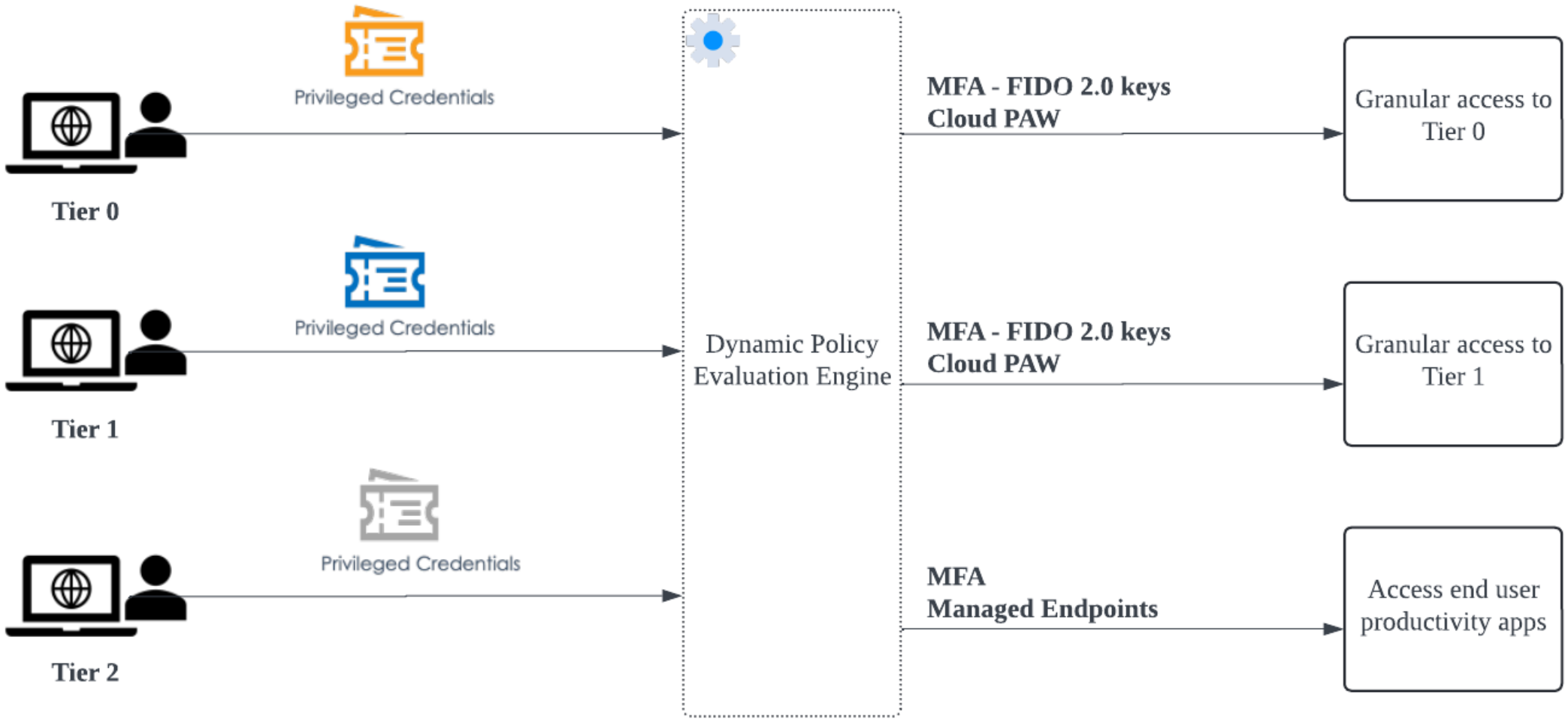
Tiering Controls for Cloud



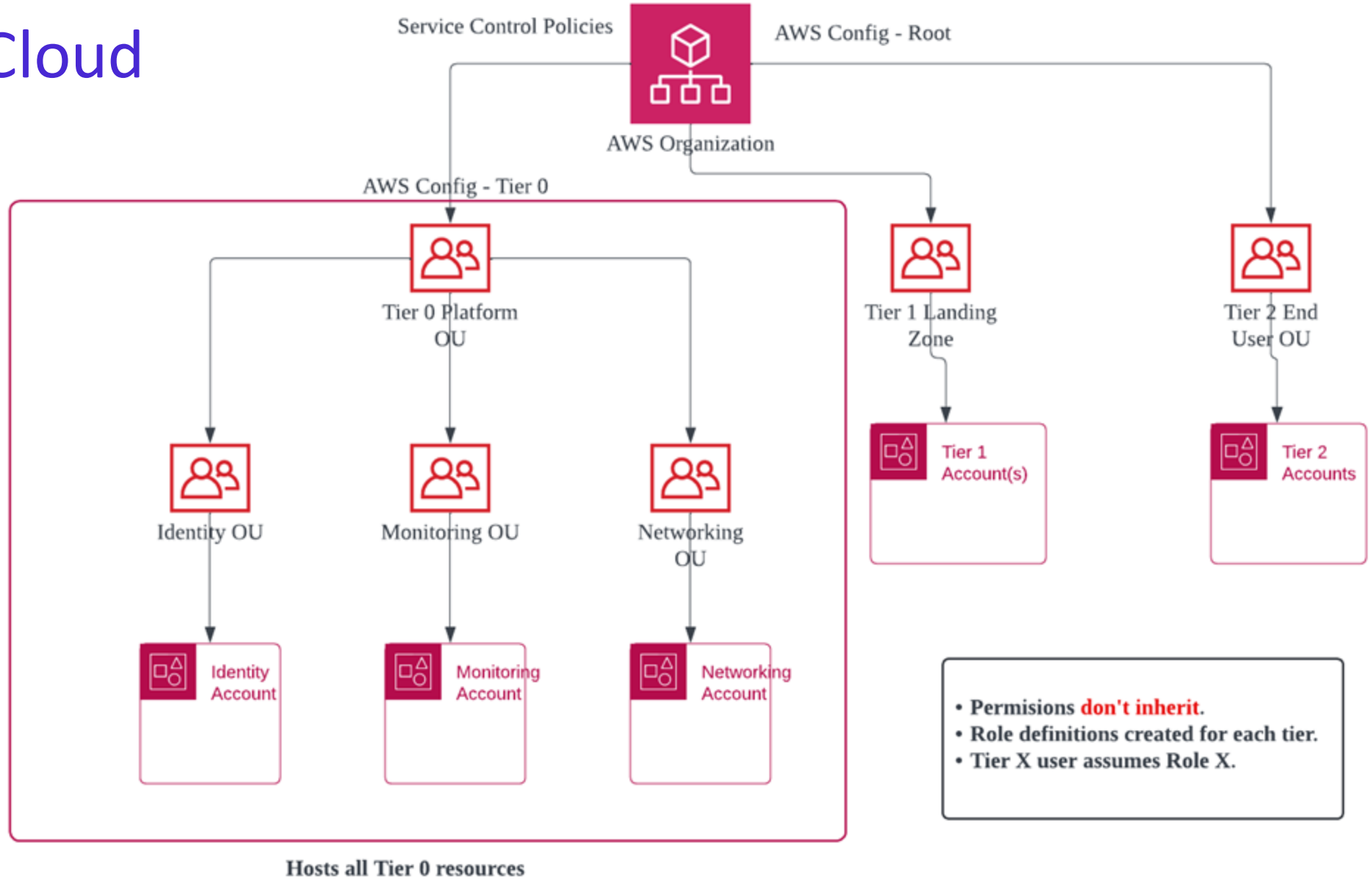


Segmentation of Resources and Network

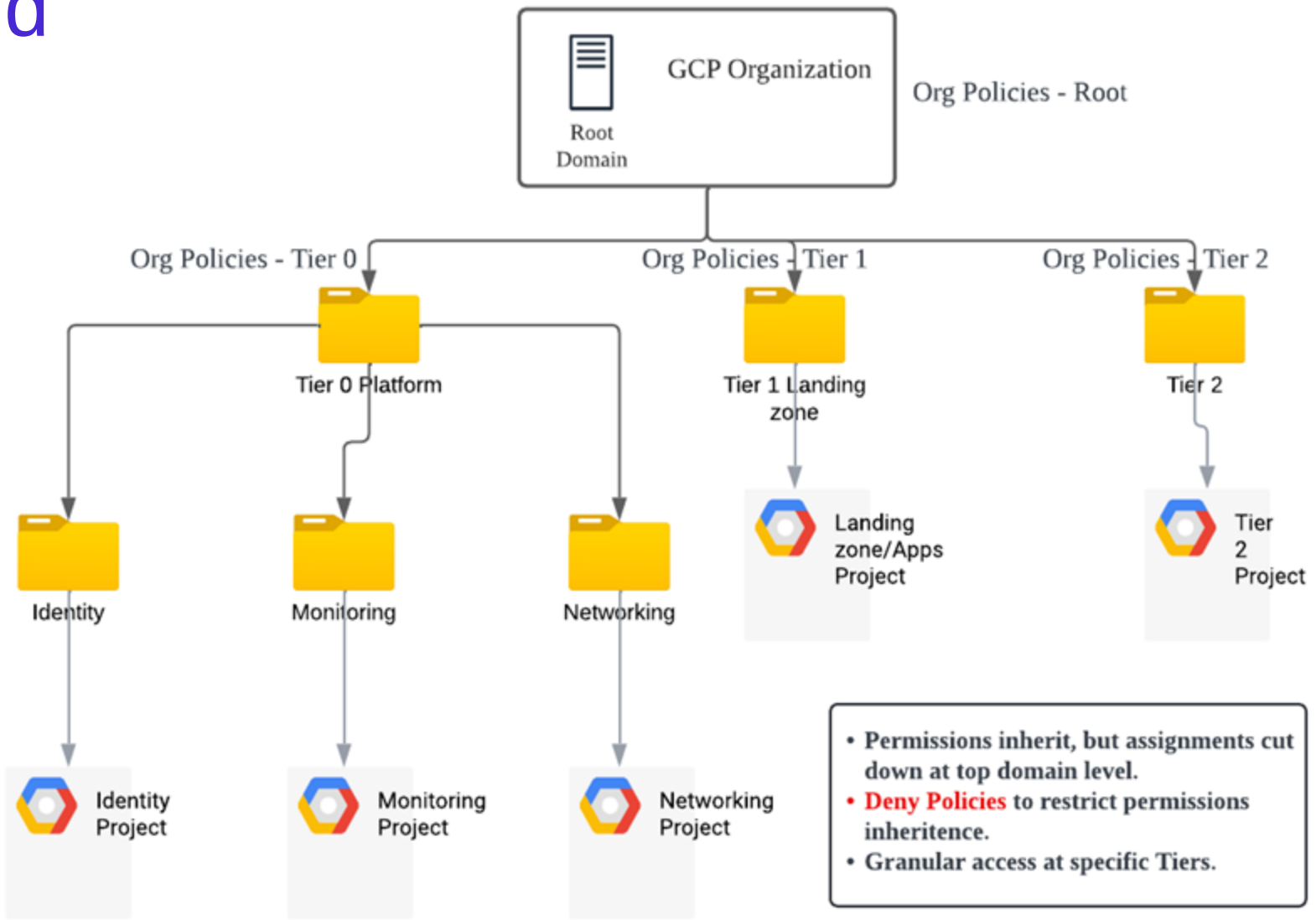
Apply Dynamic Access Controls



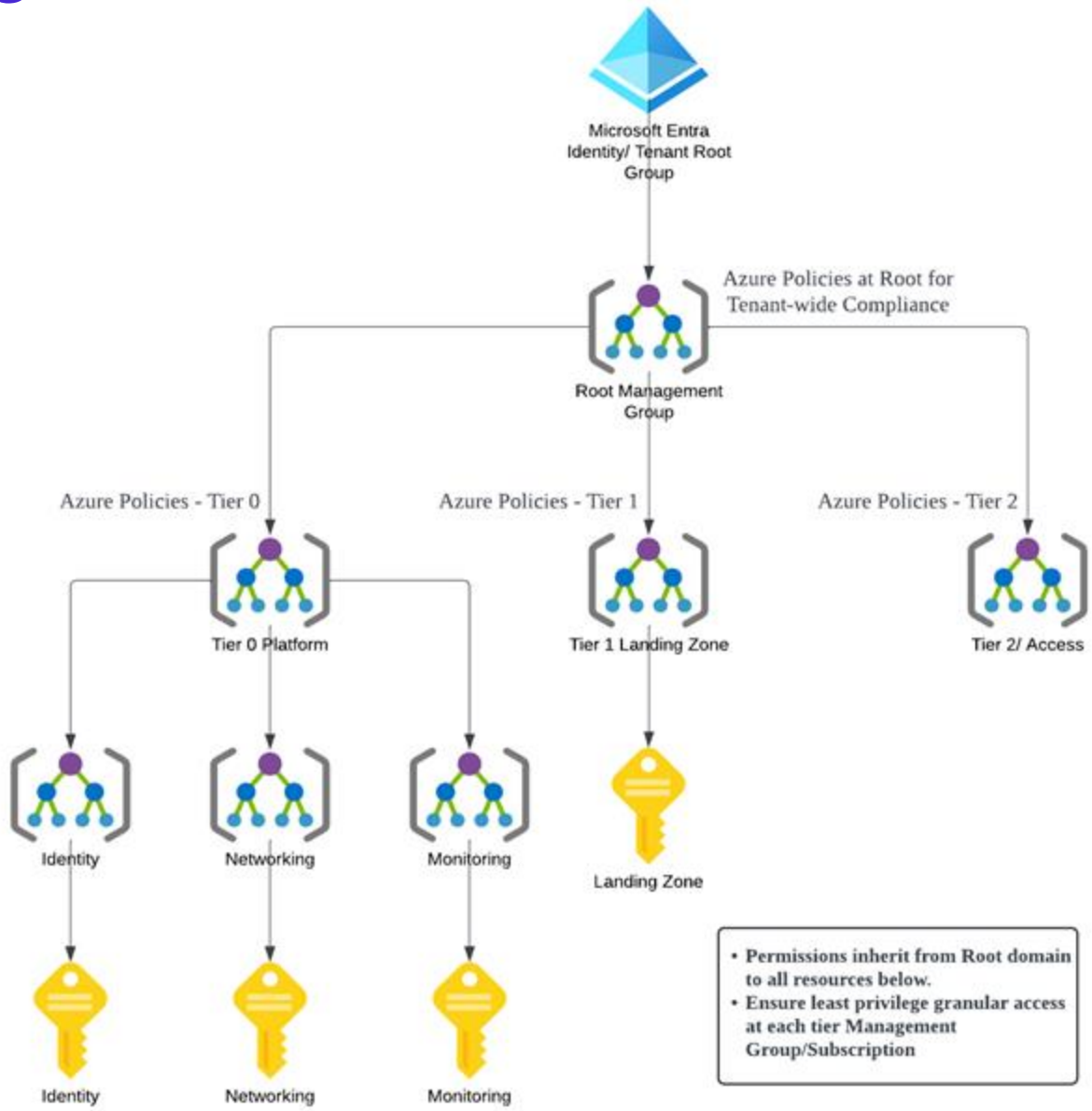
AWS Cloud


Service Control Policies
AWS Config - Root
AWS Organization
AWS Config - Tier 0
Tier 0 Platform OU
Tier 1 Landing Zone
Tier 2 End User OU
Identity OU
Monitoring OU
Networking OU
Tier 1 Account(s)
Tier 2 Accounts
Identity Account
Monitoring Account
Networking Account
• Permisions don't inherit.
• Role definitions created for each tier.
• Tier X user assumes Role X.
Hosts all Tier 0 resources

Google Cloud Platform



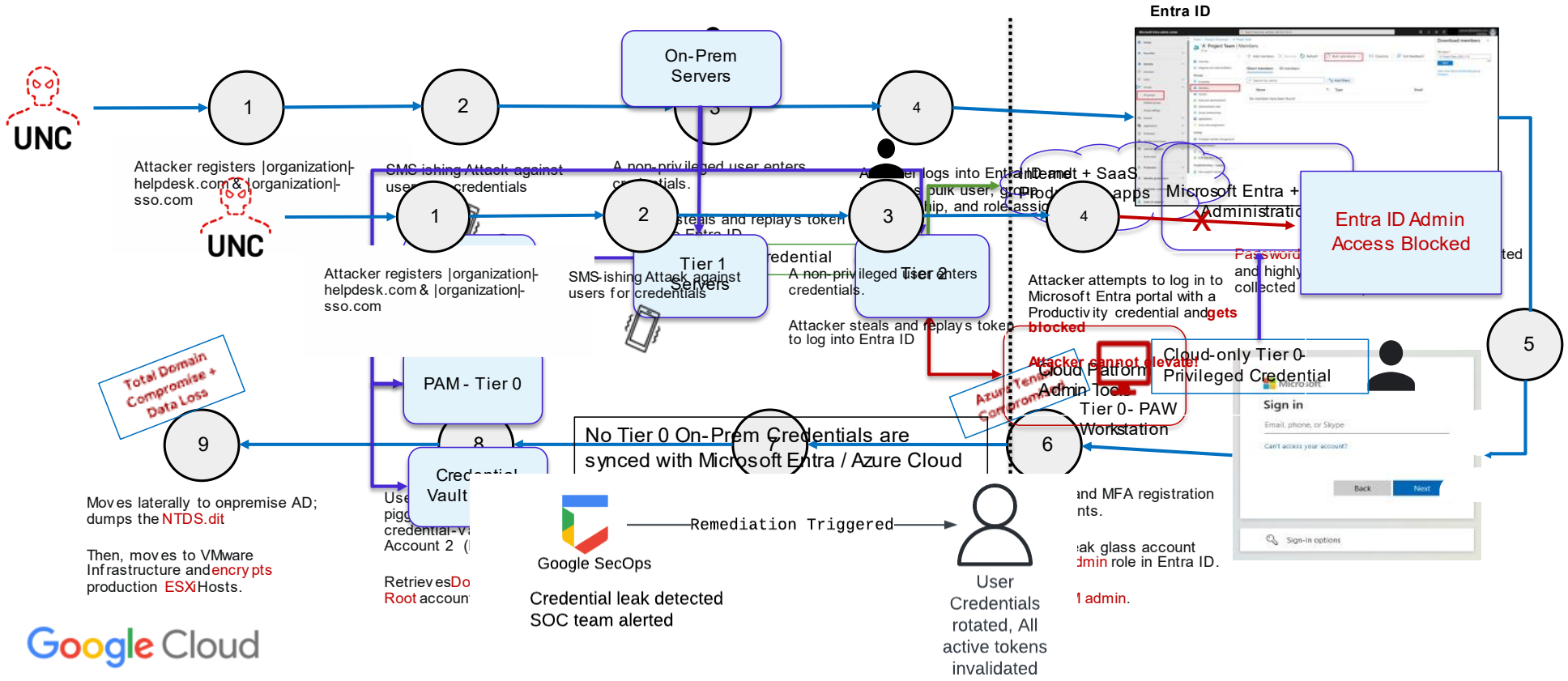
Microsoft Azure



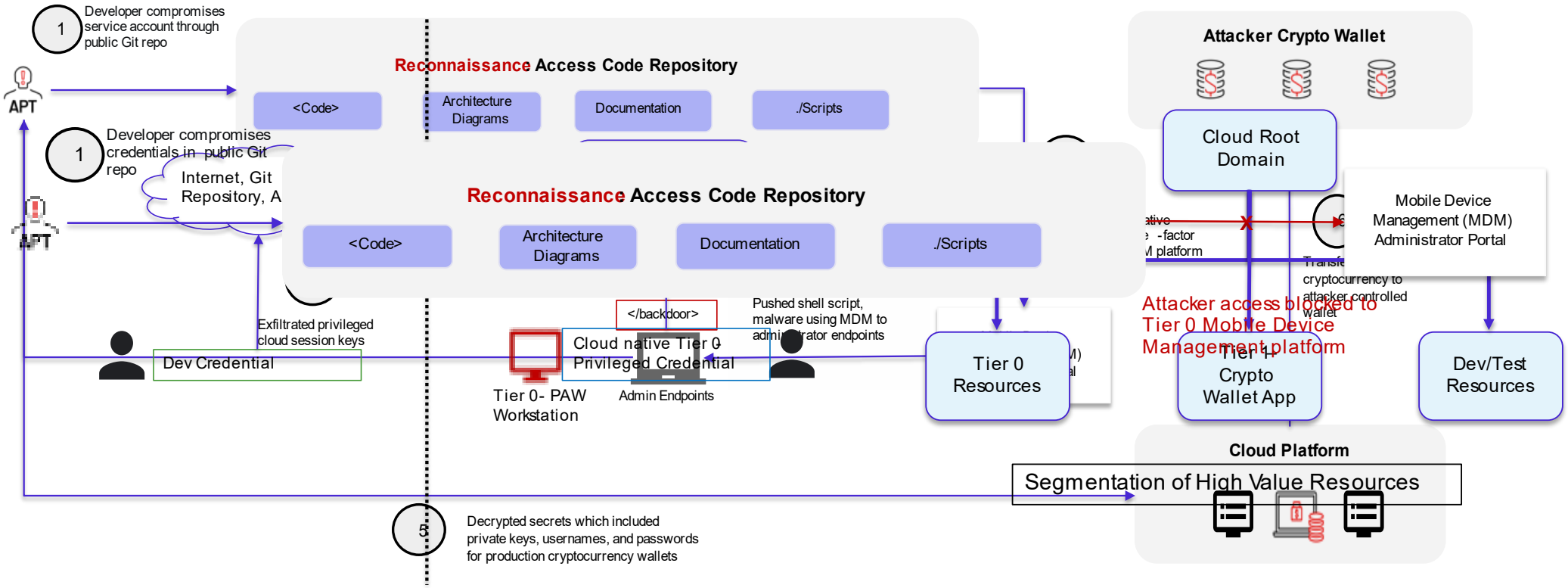
RSAC 2025 Conference

Revisit Attack Scenarios post Multi-Cloud Tiering

Scenario #1: Elevating privileges across cloud and on-prem



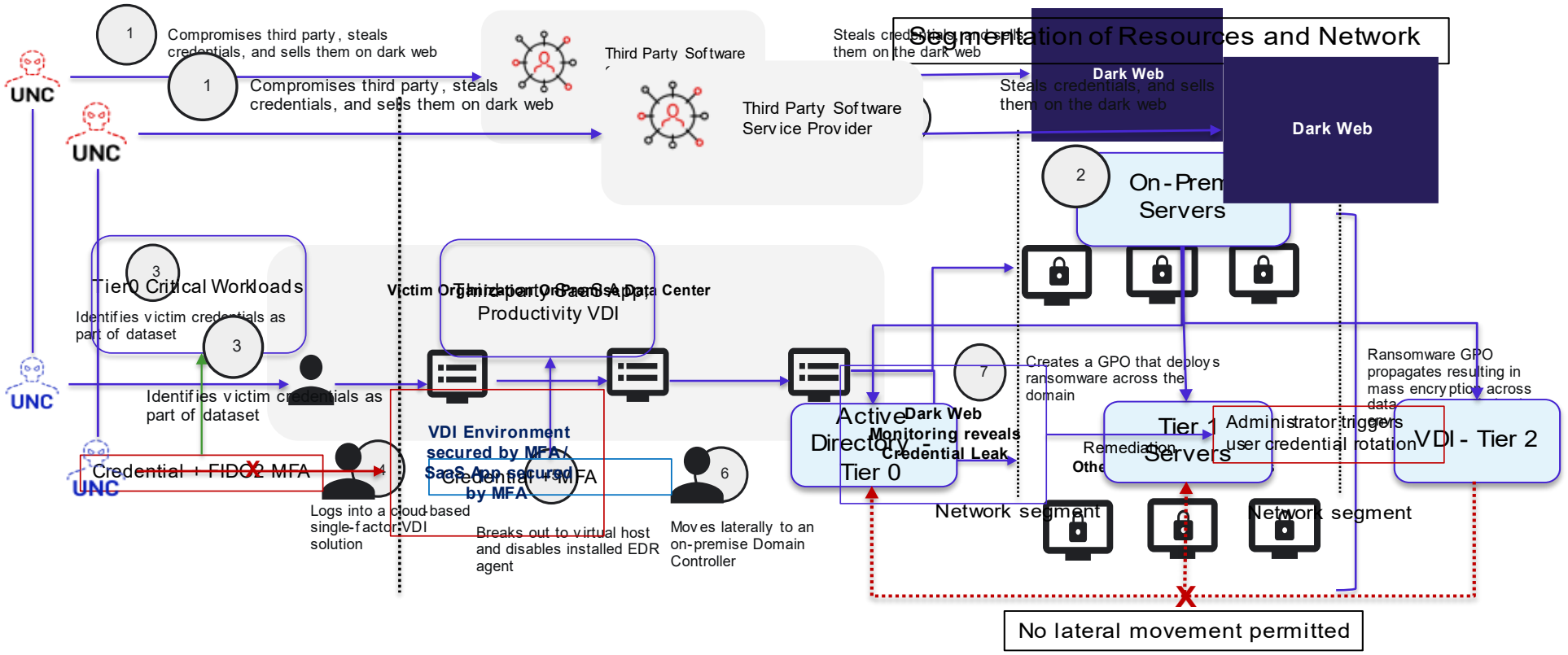
Scenario #2: Abusing Management Tooling for Cloud Access



Google Cloud

RSAC 2025 Conference

Scenario #3: Third Party tooling to Cloud Compromise


1
Compromises third party, steals credentials, and sells them on dark web
Third Party Software
Third Party Software Service Provider
Steals credentials, and sells them on the dark web
Segmentation of Resources and Network
Dark Web
UNC
2
On-Prem Servers
3
Tier0 Critical Workloads
Identifies victim credentials as part of dataset
Productivity VDI
Credential + FIDO2 MFA
VDI Environment secured by MFA/ SaaS App secured by MFA
Logs into a cloud-based single-factor VDI solution
Breaks out to virtual host and disables installed EDR agent
6
Moves laterally to an on-premise Domain Controller
Active Directory - Tier 0
Dark Web Monitoring reveals Credential Leak
7
Creates a GPO that deploys ransomware across the domain
Tier 1 Servers
Administrator triggers user credential rotation
Ransomware GPO propagates resulting in mass encryption across data
VDI - Tier 2
Network segment
No lateral movement permitted

RSAC 2025 Conference

Google – Mandiant Remediation Approach

Many Voices.
One Community.

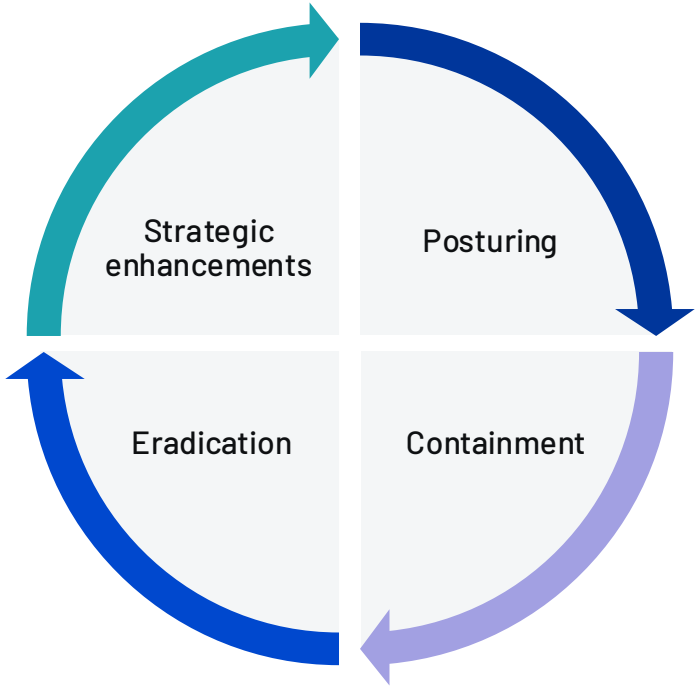
Remediation Stages

- **Part 1 - Remediate the Current Incident**

1. **Posturing**
   Provides investigative support and preparation for incident containment and eradication. *Posturing activities should not alert the attacker to the investigation.*

2. **Containment**
   Take actions to disrupt attacker activities, harden or isolate a critical service, or remove an attacker from a sensitive system or network segment (e.g., isolate and remove an attacker from critical systems or data sources).

3. **Eradication**
   Remove an attacker from the environment and implement security improvements to inhibit the attacker from quickly regaining access to the environment. *Should be performed in a concise and coordinated manner.*

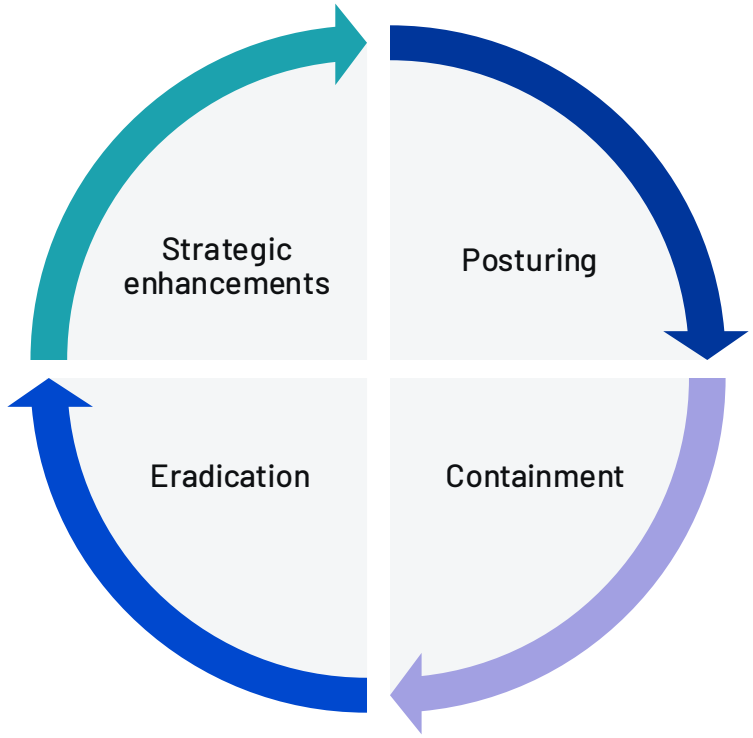


Remediation Stages

- **Part 2 – Improve security posture**

1. **Strategic enhancements**
   Provide guidance to harden the security posture by implementing strategic enhancements to the existing environment. Such enhancements can include:

   - *Tier Model for Hybrid Multi-Cloud environment*
   - *Security architecture review - Active Directory, GCP, Azure, AWS and other platforms.*
   - *Network Architecture Review*
   - *Zero Trust Security Readiness Assessment*



RSAC 2025 Conference

Many Voices.
One Community.

For more details on Tier Model for Multi-Cloud, read our whitepaper:

https://cloud.google.com/blog/topics/threat-intelligence/protecting-multi-cloud-resources-modern-cyberattacks

Apply What You Have Learned Today

- After this session you should:
  - Identify cloud platforms used by your organization
  - Document critical/non-critical workloads running on cloud
- In the first three months following this presentation you should:
  - Identify lateral movement and privileged escalation paths between different clouds and on-prem
  - Formulate a plan to identify Tier 0 resources and dependencies
  - Plan a Tier Model architecture for the cloud platforms and/or on-premises environments
- Within six months you should:
  - Drive an implementation project to implement Tier Model to segment and harden cloud platforms and on-premises connected environments

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You